Raytheon Canada Limited

Incident Management Specialist

At Raytheon Canada Limited, we are committed to both our customers and employees. Our division provides Mission Support, servicing the defence, security and aerospace sectors with a broad range of high technology products and services.

We are presently seeking a full time Cyber Security Incident Management Specialist in the Ottawa area. This role is focused on cyber security engineering activities related to the design, development, integration, test and acceptance of new and existing technologies.

Responsibilities

- Perform tasks to operate and maintain the Security Operations Center (SOC)
- Actively monitor systems and networks for intrusions
- Provide first responder services on identified security incidents
- Produce detailed incident reports and technical briefs for management, administrators and end-users
- Develop a procedural set of responses to security problems
- Configure and use intrusion detection systems, firewalls, content checkers and antivirus software
- Collect, collate, analyze and disseminate threats and vulnerabilities information
- Analyze and support manage cyber security system requirements for systems involving multiple technologies and subcontractors
- Review cyber security engineering related documentation (specifications, interface control documents, test requirements, test plans) in support of integration, verification and validation of technology baselines
- Perform trade studies and make recommendations with respect to insertion of cyber security technologies to meet required capability updates and upgrades
- Perform job analysis to estimate incident management effort required for specialized SOC tasks.
- Responsible for ensuring that SOC tasks are performed in accordance with our customers' engineering policies and procedures
- Collaborate with the Cyber Security team on SOC system level requirements definitions and changes and support the Cyber Security Specialists to integrate the system security requirements
- Work within an Integrated Product Development team (IPT) to:
    - Develop and maintain security architecture in accordance with security technical standards
    - Perform ongoing cyber vulnerability assessment and system hardening
    - Support engineering and maintenance of technical security safeguards
    - Develop and maintain Security Assessment and Authorization documentation
    - Provide cyber monitoring and incident response services

Requirements

- Must have more than 5 years of previous experience in systems engineering, electrical engineering, computer engineering, telecommunications, information systems or computer science
- A University undergraduate degree in engineering, computer science, or equivalent, or a College diploma (two or three year program) in an electrical engineering, electronics, telecommunications, computers or information technology program is required
- Must be capable of obtaining an industry recognized certification in the area of specialization (i.e. Cisco CCNA Security, SANS GIAC, Security+…)
- Demonstration of work experience in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems operations is desired
- Experience in security operation center work including experience in actively monitoring systems and networks for intrusions, producing detailed incident reports and technical briefs for management, administrators and end-users, and developing a procedural set of responses to security problems is required
- Requires a combination of education and experience in:
    - Use of network scanners and vulnerability analysis tools
    - Reporting and resolving IT Security incidents
    - Understanding Networking Protocols such as HTTP, FTP, Telnet, TCP/IP, DNS, SMTP, SNMP
    - Understanding networking security protocols such as SSL, S-HTTP, SMIME, IPSec, SSH,
    - Configuring and using intrusion detection systems, firewalls, content checkers and antivirus software
    - Monitoring network infrastructure components such as multiplexers, routers and switches
    - Providing incident analysis support and producing system activity reports
    - Collecting, collating, analyzing and disseminating threats and vulnerabilities information
    - Conducting on-site reviews and analysis of system security logs

Other information:

Only those selected for an interview will be contacted. Interviewed candidate will be required to successfully complete a Criminal reference check and pass a security clearance check to a secret level through the Canadian Government.

Please forward your cover letter and resume stating file number W2017-023 to:

Raytheon Canada Limited
Attn: Human Resources
919 72nd Ave, N.E.
Calgary, Alberta
T2E 8N9
Email: HR@Raytheon-ssd.com
Fax: (403) 295-6682

Raytheon Canada Limited is proud to be an equal opportunity employer and welcomes a wide diversity of applicants.

We thank all candidates for applying. We will only contact candidates selected for further consideration. If you are invited to continue in the selection process and require any form of accommodation, please notify us. Accommodations are available for candidates taking part in all aspects of the selection process.